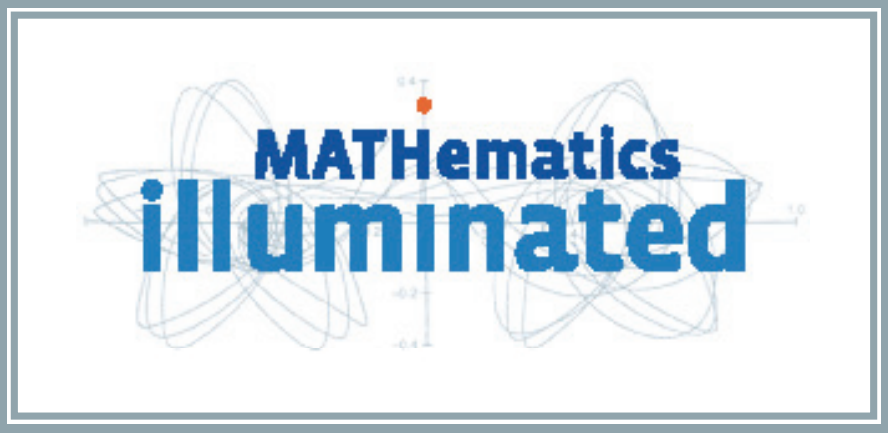


TEXTBOOK

UNIT 1

UNIT 01

THE PRIMES

TEXTBOOK

UNIT OBJECTIVES

- Primes are the fundamental building blocks of arithmetic.
- There are infinitely many prime numbers.
- The fundamental theorem of arithmetic says that each whole number can be uniquely decomposed into a product of primes.
- The answer to whether or not there is a pattern behind the primes has eluded mathematicians for millennia.
- One can find arbitrarily long “prime deserts” on the number line.
- One can find finite arithmetic sequences of primes of any length.
- Clock math is a way of generalizing arithmetic.
- Primes and clock math can be used together to create strong encryption schemes.

“”

Reason is immortal, all else mortal.

PYTHAGORAS

“”

Mathematicians have tried in vain to this day to discover some order in the sequence of prime numbers, and we have reason to believe that it is a mystery into which the human mind will never penetrate.

LEONHARD EULER

SECTION 1.1

INTRODUCTION

In 1974, astronomers sent a message into space from the Arecibo radio telescope in Puerto Rico in an attempt to broadcast the presence of our intelligent life to any other potentially sentient beings that happened to be listening. The message contained information about our planet's location, the basis of our chemistry, and rudimentary information about our biological form. In sending this message, astronomers had to confront a deep problem: how does one communicate with another intelligent species that one knows nothing about?

At the time, astronomers thought that the best way to ensure the comprehensibility of the message was to use a concept fundamental to our own logical understanding of the world, namely, prime numbers. No known natural process creates prime numbers, yet they are at the very center of mathematical thought. The astronomers assumed that any beings intelligent enough to be able to listen to radio broadcasts would know about prime numbers. With this in mind, the message senders encoded a pictogram consisting of 1,679 bits; although the number 1,679 is not itself prime, it is the product of two prime numbers. The general idea was that any alien listener who receives a random number of blips might think to factor that number, just to get a sense of what it is. Choosing a number whose only factors are two primes might prompt the receiver to think "two-dimensional," a rectangular array, in other words, with one factor representing the number of rows and the other representing the number of columns. Using this information to arrange the pixels into a rectangle would reveal the picture. This, of course, assumes that an intelligent alien would recognize prime numbers to be special in some way.

Item 1671 / Frank Drake, ARECIBO MESSAGE OF 1974 (1974). Courtesy of Frank Drake.

This assumption is actually quite reasonable. Prime numbers, known to humankind for at least 20,000 years, represent a fundamental concept of mathematics that has provided rich grounds for study. Primes have been described as the atoms of arithmetic, the indivisible parts from which all other numbers can be constructed. Seemingly simple, they have provided some of the most challenging problems

SECTION 1.1

INTRODUCTION
CONTINUED

for those willing to explore their world. Long studied for their mysteries, many of which remain unsolved, primes were, until relatively recently, solely the concern of mathematicians. With the explosion of digital communications and our dependence on Internet transactions, however, primes now play a pivotal role in other areas, as well.

The advent and growth of the Internet and the "information age" have given unprecedented convenience to millions of technology users worldwide. Technological advances and their application in numerous fields have helped to shrink perceived distances and have done much to break down barriers that divide us. Peril often accompanies progress, however, and our modern Internet economy is not immune to risks. For example, when we make a purchase, pay bills, or check our bank balance online, how do we know that someone will not intercept the transmission and steal our personal information? One of the ideas we will see in this unit is how the properties of prime numbers, in combination with modular arithmetic, or "clock math," are used to help keep our information secure.

In this unit we will see how primes are fundamental to mathematical thought. We will explore the seemingly simple concept that underlies their existence, and we'll catch a glimpse of the mystery inherent in their distribution on the number line. Finally, we'll take a brief look at how the modern standard of data security, RSA encryption, uses fundamental properties of primes to create virtually impenetrable codes.

SECTION 1.2

MATH AT THE DAWN OF TIME

- Tally Sticks
- Cultural Math

TALLY STICKS

- The earliest evidence of humans using numbers comes in the form of tally sticks.
- The Ishango bone represents a level of early mathematics more sophisticated than simple counting.

Evidence suggests that the exact beginning of mathematical thought, even the origin of the concept of a "number," predates the advent of written language. The earliest example of recorded mathematical symbols is a sequence of tally marks on the leg bone of a baboon found in Swaziland, dating to around 35,000 years ago. By contrast, the earliest known language writings date to around 6,500 years ago. It is not known for sure what the tally marks on the bone represent, but it is plausible that they represent a record of an early hunter's kills. These tally marks may represent numbers in application, but there may also be evidence that early humans were interested in properties of numbers themselves.

Item 3060 / Oregon Public Broadcasting, created for *Mathematics Illuminated*, ISHANGO BONE (2008). Courtesy of Oregon Public Broadcasting.

Possible evidence of mathematics more sophisticated than counting comes from another bone dated ten thousand years younger than the Swaziland counting bone. Around 25,000 years ago, by the shores of Lake Edward (which today lies on the border between Uganda and Zaire), the Ishango people lived in a small fishing, hunting, and farming community. This settlement lasted for a few centuries before being buried in a volcanic eruption.

SECTION 1.2

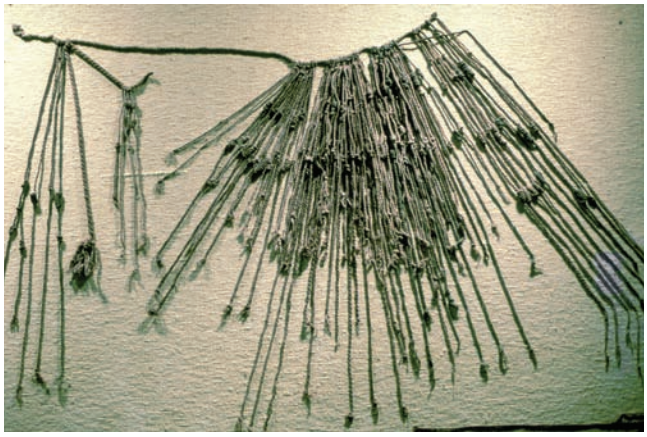
MATH AT THE DAWN OF TIME
CONTINUED

Excavations at this site turned up a bone tool handle with a series of interesting marks. The Ishango bone, as it is now called, has groups of markings, some of which represent primes. Although the exact meaning of these markings is still being debated, the current thought is that they represent some sort of lunar calendar. Regardless of the precise meaning of the markings, the artifact demonstrates that humans were thinking about mathematical concepts, perhaps even the concept of prime numbers, 25,000 years ago, well before the emergence of cities.

CULTURAL MATH

- Mathematics arose independently in different forms across many cultures throughout history.

Jump 10,000 years forward and a bit to the east from the makers of the Ishango bone, and you're in the emerging Egyptian and Fertile Crescent civilizations. These civilizations had deep understanding of mathematics and used it to achieve unequalled engineering feats. Babylonian clay tablets show an understanding of Pythagorean triples, centuries before the cult of Pythagoras appeared in Greece.



Item 2251 / Inca, QUIPU. USED FOR COUNTING (fifteen-early sixteenth century). Courtesy of Kathleen Cohen.

Item 2250 / Babylonian, MATHEMATICS TABLET SHOWING CALCULATIONS OF VOLUME (ca. 1635 BCE). Courtesy of Kathleen Cohen.

However, these were not the only ancient civilizations to develop, presumably independently, familiarity with numbers and number relationships. Mathematical concepts may have spread naturally throughout Africa, and the Middle East, and Asia, but they also appeared early on in Central and South America.

Evidence suggests that the development of mathematics in early cultures was tied to

SECTION 1.2

MATH AT THE DAWN OF TIME
CONTINUED

Item 2253 / Mayan, CALENDAR RELIEF (fifth-ninth century). Courtesy of Kathleen Cohen.

specific purposes. Much of early mathematical thought was focused on representing and understanding the movements of the heavens, as is evident in the Mayan long count calendar and the constellations of the zodiac. Elsewhere, such as in ancient China, mathematics was put to use in bookkeeping and other business activities. Math's development generally served practical purposes until about 600 BC, when the Greek philosophers began to explore the world of numbers itself.

SECTION 1.3

NUMBER FOR NUMBER'S SAKE: THE GREEKS

- Playing with Numbers
- The Primacy of Proof
- Figurate Numbers

PLAYING WITH NUMBERS

- The Greeks studied numbers independent of their application to uses in the real world.

Prime numbers may have been of interest to the people of Ishango, but it was the Greeks who began to ask deep questions about them. The Greeks held high esteem for the pursuit of knowledge and, in particular, mathematical truth. One would not have expected such a high-level fascination from the illiterate and innumerate people who conquered the Aegean peninsula. Their conquests and the knowledge that flowed along their trade routes, however, enabled them to catch up quickly with the rest of the mathematical world.

While the rest of humanity was seemingly occupied with the more practical uses of mathematics, the Greeks were among the first to develop a mathematical world that was not necessarily tied to real-world applications. It was during this time that the concept of axiomatic structure emerged—mathematical proof, in other words. Thales, a mathematician who is said to have astonished his countrymen by correctly predicting a solar eclipse in the year 585 BC, is generally credited as taking the first steps toward focusing on the logical structure and principles behind mathematics. Described as the first philosopher and the first mathematician, he is definitely the first person to whom a specific mathematical "discovery" is ascribed, namely that an angle inscribed in a semi-circle is a right angle. As is often the case with the emergence of new ideas, there is some dispute on this, however. Thales is generally given the credit for this discovery, although some claim that he simply re-packaged a previous Babylonian finding.

There is some debate as to whether it was Thales or the Pythagoreans who presided over the shift in mathematics from practical concerns to the development of general principles and ideas. The supposed motto of the Pythagorean group, "All Is Number," encapsulates their preoccupation with both mathematical and numerological concepts. For example, they ascribed a gender

SECTION 1.3

NUMBER FOR NUMBER'S SAKE: THE GREEKS
CONTINUED

to numbers, odd numbers being male and even numbers being female. Much of the mathematical tradition of ancient Greece, and, thus, of the civilizations that followed, stemmed from the obsessions of the Pythagoreans.

THE PRIMACY OF PROOF

- Proof has long been one of the central ideas in mathematics.
- Mathematical theorems, unlike scientific theories, last forever.

Chief among the Pythagorean concerns was the notion of proof. In philosophy it was possible to argue, as the Sophists did, both sides of a scenario and see that neither was a clear winner. Math, however, is different in that "truth" can be proved through a system of assumptions and allowed actions that show that a given statement must follow from initial postulates. In other words, in mathematics at least, there is indisputably a right answer, although it may not always be obvious. This clarity, and the comfort that it often brings, was of central importance to the Pythagoreans, and it represents a distinguishing feature of the field of mathematics.

Theorems proved by, or at least attributed to, early Greeks, such as the Pythagoreans, remain as true today as they were in ancient times. The same cannot be said for any host of other Greek beliefs from non-mathematical disciplines. One of the alluring features of mathematics is that it enables one to say definite things about reality. This aspect was, and continues to be, a major reason why people choose to study mathematics.

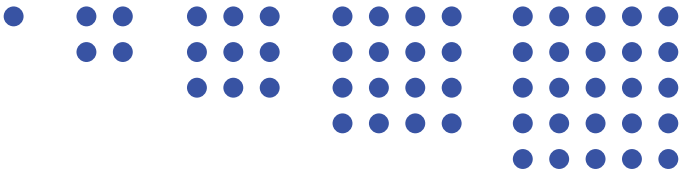
FIGURATE NUMBERS

- Playing with the geometric structure of numbers led to early insights in number theory.

Playing with numbers—the exploration of numbers for their own sake—is perhaps the first step towards mathematical sophistication. The Greeks were fascinated by the different properties that certain numbers exhibited geometrically. If we represent each whole number by a collection of pebbles equal in count to that number, then many interesting relations and properties of numbers can be found by looking at the shapes that one is able to make with different arrangements of the collections.

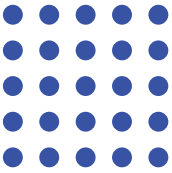
SECTION 1.3

NUMBER FOR NUMBER'S SAKE: THE GREEKS
CONTINUED



Square numbers are whole numbers that, when represented as a collection of pebbles, can form a square array. The first square number is 1, the second is 4, which can be portrayed as a 2×2 array, the third square number, 9, forms a 3×3 array, etc. The triangular numbers can also be represented by an interesting sequence of dot patterns, which is, in fact, the basis of their classification as "triangular" numbers.

The squares and triangular numbers, in this context, are examples of "figurate" numbers—numbers that have "shapes." Figurate numbers hold many interesting properties; for example, consider the 5×5 square.



Is it evident that the fifth square number, 25, represents the sum of the first five odd numbers?

We can decompose the square into nested L-shapes, also called gnomons, as shown above. It is, hopefully, straightforward to state that any square can be

SECTION 1.3

NUMBER FOR NUMBER'S SAKE: THE GREEKS
CONTINUED

broken down in this way. It should also be clear that every gnomon represents an odd number, and that nested gnomons represent consecutive odds. Adding a gnomon to an n $\times$ n square increases the dimensions to (n+1) $\times$ (n+1), which is still a square. It is reasonable, then, to conclude that the sum of the first n odd numbers is n^2.

In the online interactive, you will have the opportunity to play with figurate numbers, such as those we have discussed, and to discover interesting relationships between them. The study of figurate numbers leads quite naturally to primes, which we will investigate further in the next section.

SECTION 1.4

PRIMES

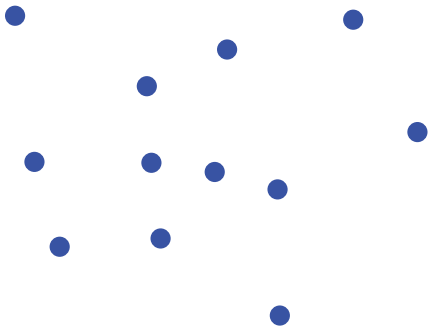
- Rectangles
- Factor Trees
- Fundamental Theorem of Arithmetic

RECTANGLES

- The rectangle model of multiplication links a number's geometric structure to its divisors.
- Primes are numbers that cannot be represented by rectangles with both dimensions whole numbers greater than one.

Exploring a number's geometric shape leads quite naturally to the notion of prime numbers. Just as before, we can consider a whole number to be a collection of pebbles. We could then address the question of whether it is possible to form a rectangle with the pebbles.

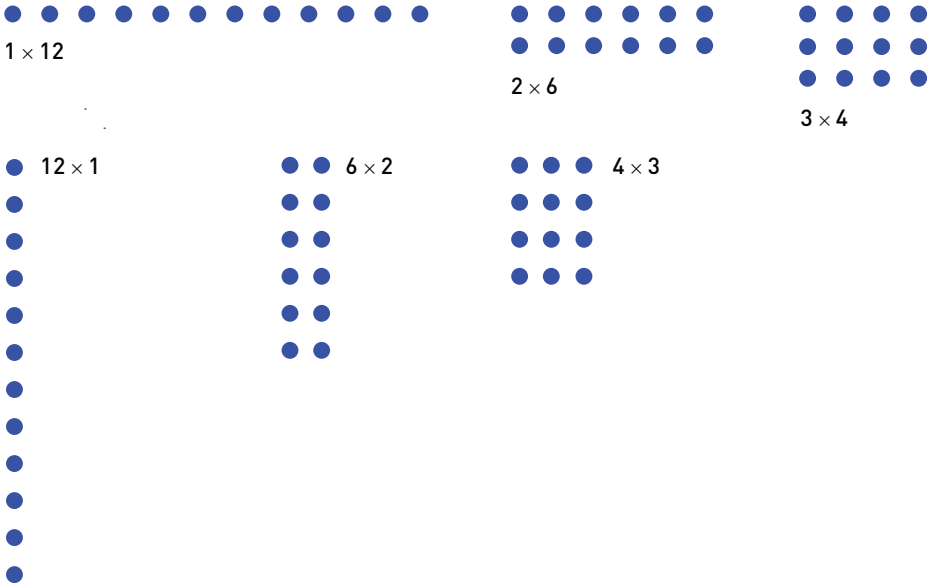
Let's look at a collection of 12 pebbles:



SECTION 1.4

PRIMES
CONTINUED

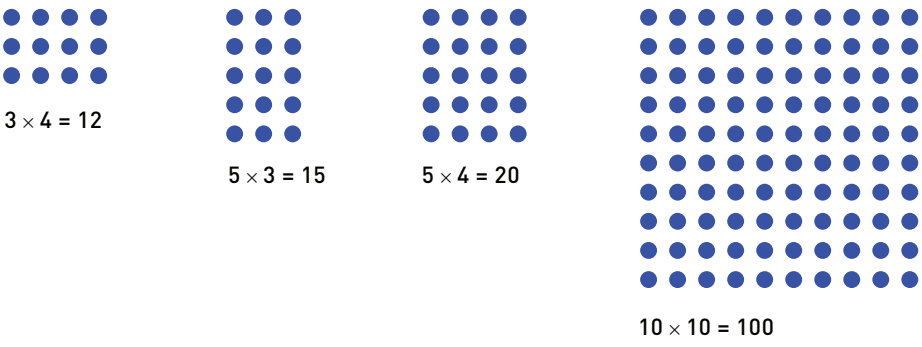
We can arrange these 12 pebbles into various rectangular arrays.



Note that the dimensions of each rectangle—the height and width—multiply to equal 12. We call each of these numbers representing a possible dimension a "divisor" of 12; so 12 has six divisors: 1, 2, 3, 4, 6, and 12. In general, we say that *a* is a divisor of *N* if for some whole number *b*, $a \times b = N$.

Note that any whole number, *N*, can be represented by a $1 \times N$ rectangle—a single row of pebbles.

Some numbers, such as 12, 15, 20, and 100, can be represented by rectangles that are more interesting than a single row of pebbles.



SECTION 1.4

PRIMES
CONTINUED

Other numbers, however, such as 5, 11, 17, and 101, can be represented only by the single-row type of rectangle.

$1 \times 101 = 101$

$1 \times 17 = 17$

$1 \times 11 = 11$

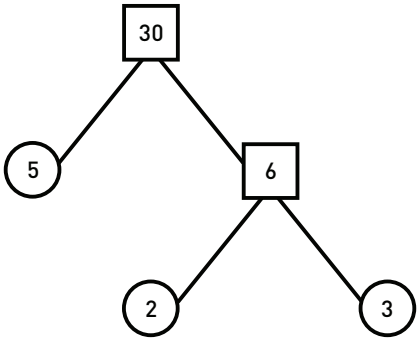
$1 \times 5 = 5$

In arithmetic, we call a number "prime" if it has precisely two divisors. These primes are the numbers, such as 2, 3, 5, 7, and 11, whose pebble representations can be arranged only into the single-row type of rectangle. Numbers with more than two divisors are called "composite." Geometrically, these are numbers that can be represented in dot formations by more than one type of rectangle. Note that the number one, which has precisely one divisor, is considered to be neither prime nor composite.

FACTOR TREES

- Factor trees reveal the prime decompositions of composite numbers.

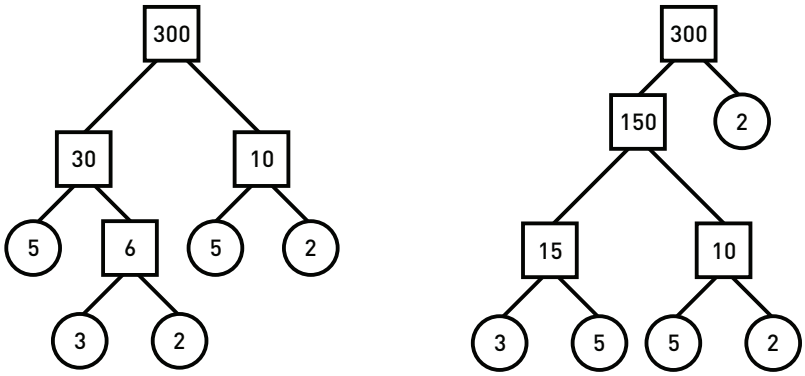
A number that is prime has exactly two divisors, itself and one. If a number is not prime—composite, in other words—we can "factor" it to find all of its constituent prime "factors." For example, the number 30 can be written as 6×5, which can in turn be written as a product of all-prime factors: $2 \times 3 \times 5$.



Some numbers have multiple possible factor trees. Let's consider the number 300, for example:

SECTION 1.4

PRIMES
CONTINUED



Note, however, that although these factor trees for 300 are different, the set of prime factors generated is the same: 3, 5, 5, 2, and 2.

Any composite number can be decomposed this way into a product of primes. In doing this, we see that primes can indeed be thought of as the "atoms," or fundamental building blocks, of all numbers. Real atoms are the smallest individual pieces of an element, such as gold, that still retain all the properties of that element. In this analogy, a composite number is like a molecule. Breaking apart a molecule generates a collection of atoms of different elements, each of which cannot be broken down further. We perform an analogous breakdown when we decompose a composite number and express its prime decomposition via a factor tree. It is interesting to note that every composite number breaks down into a unique product of primes. How do we know this?

FUNDAMENTAL THEOREM OF ARITHMETIC

- The Fundamental Theorem of Arithmetic states that every number has only one prime decomposition.
- Primes are the "atoms" of arithmetic.

The fact that every composite number has a unique prime decomposition, a concept known as the fundamental theorem of arithmetic, is often taken for granted. In mathematics we should always be careful to question both our own assumptions and the assumptions of those who would tell us something. Such a questioning attitude derives from the previously mentioned importance of proof, pioneered by the Greek philosophers, logicians, and mathematicians. The tools for proving the fundamental theorem of arithmetic were first laid down by the great mathematician Euclid, who lived in Alexandria in the third century BC. These core concepts were not rigorously expressed, however, until Karl Gauss

SECTION 1.4

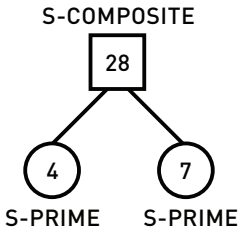
PRIMES
CONTINUED

put them on a solid foundation in his *Disquisitiones Arithmeticae*, first published in 1801. Expressed in modern language, the fundamental theorem of arithmetic states that:

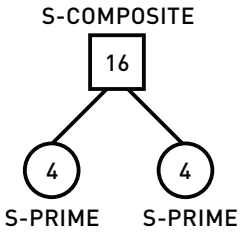
Every natural number greater than 1 can be written as a product of prime numbers in essentially just one way.

This may seem intuitive, even obvious, but it doesn't have to be the case. We can imagine a number system in which the fundamental theorem of arithmetic does not hold. Take, for example, a set, S, consisting of the numbers {1, 4, 7, 10, 13, 16, 19,..., 3n+1,...}. Each number in this system is one more than a multiple of three. Suppose that these numbers are all we have to work with in performing arithmetic operations in this system. As with the natural numbers, we can have a notion of prime and composite in this system—let's call them "S-prime" and "S-composite" respectively.

S = {1, 4, 7, 10, 12, 16, ... 3n+1}



The "S-Prime" factorization of 28.

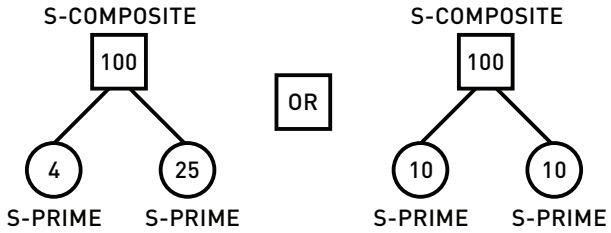


The "S-Prime" factorization of 16.

The number 10 has only two divisors in this system, one and itself. The number 16, on the other hand, has three: 1, 4, and 16. Numbers such as 4, 7, and 10 can be called "S-prime," because they have exactly two divisors within the number system, S. Numbers such as 28 and 16 can be called "S-composite," because they have more than two divisors in S. If S obeys the fundamental theorem of arithmetic, then no matter how we draw a factor tree for an S-composite, we should end up with the same set of S-primes. Is this the case? Let's look at two factor trees of the S-composite number 100:

SECTION 1.4

PRIMES
CONTINUED



$100 = 4 \times 25$
An "S-Prime" factorization of 100.

$100 = 10 \times 25$
A different "S-Prime" factorization of 100.

Notice that 100 can be written as a product of S-primes in two different ways, 4×25 and 10×10. So, this demonstrates that the fundamental theorem of arithmetic does not hold for our number system S. This suggests to us that we cannot take this seemingly obvious property of natural numbers for granted—hence, Gauss's proof that every natural number greater than one has a unique prime factorization is of great importance in the field of number theory.

Actually, finding a number's prime decomposition—also known as the prime factorization—is relatively straightforward, provided we are aware that our number is divisible by some factor and we know what that factor is. Suppose, however, that we come across some large number and wish to find its prime factors. How would we do this? How would we know whether it even had prime factors other than itself?

If the situation were different, and we wished to multiply two large numbers, our task would be easy—we have good, efficient algorithms for multiplying numbers of any size. Factoring a large number, however, is exceedingly difficult. Most factoring methods involve some version of the "trial and error" strategy. Even for a relatively small number, such as 527, our only real choice is to try dividing it by potential factors until one of them divides it evenly. In this case, it wouldn't take us too long to find that $527 = 17 \times 31$. For a very large number, however, going through all the possibilities could take an intractably long time.

If someone took two large prime numbers and multiplied them together and then asked us to find the prime factorization of that composite number, we would be in trouble. The number we are given has only two prime factors, and if we don't know either of them, there is no good algorithm for finding them. This "one-way-street" aspect of multiplication and factoring will play a key role in

SECTION 1.4

PRIMES
CONTINUED

our upcoming discussion of encryption. Before we tackle encryption, however, we should take a closer look at prime numbers, for they themselves hold a great deal of mystery.

SECTION 1.5

QUESTIONS ABOUT PRIMES

- An Infinitude of Primes
- Is It Prime?
- Structure of the Primes
- Riemann's Hypothesis

AN INFINITUDE OF PRIMES

- Euclid proved that, given a finite list of primes, one can always create a new prime not on that list, which implies that there are an infinite number of primes.

Let's take a look at a partial list of primes, with spaces left to represent the composite numbers that occur between them:

_2 3 _ 5 _ 7 _ _ _ 11 _ 13 _ _ _ 17 _ 19 _ _ _ 23 _ _ _ _ _ 29 _ 31 _ _ _ _ _ 37 _ _ _ 41 _ 43 _ _ _ 47 _ _ _ _ _ 53...

The primes seem to be haphazardly distributed; that is, there is not a clear pattern to them. It seems also, with the exception of the occasional pair of "twin primes"—primes separated by only one number-- that the gaps between adjacent primes generally tend to become larger as the numbers themselves get larger. From this evidence, one could plausibly think that at some point the stream of primes dries up and that there might be no primes above some given number. The question of how many primes there are is an interesting one that arises quite naturally. Is the list finite or infinite?

Euclid thought about this problem and found a way to show that, in fact, there are an infinite number of primes to be found. He did this by demonstrating that from any finite collection of primes it is always possible to find one more. For example, take the finite set {2, 3, 5}. Euclid suggested multiplying all members of the set together and adding one. For our set, this gives us 31 ($2 \times 3 \times 5 + 1 = 31$), which cannot be evenly divided by any of the primes on our list, for it always gives a remainder of one. Hence, 31 is a "new" prime.

Remember that in math it's good to keep a skeptical, questioning attitude concerning pronouncements. Perhaps that example was just an anomaly, and maybe 2, 3, 5, and 31 are the only primes that exist. Applying Euclid's test strategy to this expanded set, we would multiply them together and get 930, to

SECTION 1.5

QUESTIONS ABOUT PRIMES
CONTINUED

which we add one to end up with 931. Dividing 931 by 2, 3, 5, or 31 always leaves a remainder of one. Does this mean that 931 is prime? No, not necessarily, but it does mean that none of the numbers 2, 3, 5, and 31 is a factor of 931. It might not be obvious, but 931 is actually the product of 7, 7, and 19. So, even though 931 is not itself prime, it is a composite number whose prime factorization reveals new prime numbers (7 and 19) not in our original list. Again, our list was incomplete.

The point is that Euclid showed that multiplying together a finite list of primes and adding one will always produce a new number which, if not itself prime, factors into new primes not on the list. We can always find a new prime using this method. This implies that any finite list will never include all of the prime numbers; therefore, the list of primes must be infinite!

The method we employed above will always uncover at least one new prime, but it could very well miss some along the way. In our first example above, we missed a few primes in between 5 and 31, namely 11, 13, 17, 23, and 29. This method obviously will not produce an exhaustive list of primes; it serves only to generate a new prime or two, given a list of starting primes.

In the second example above, we found that this method produces a number that may not necessarily be prime. This suggests to us that it would be nice to have an efficient, fail-safe method for determining whether a number of any size is prime or not.

IS IT PRIME?

- Determining whether or not a number is prime is a non-trivial task.

The most straightforward way to know for sure whether or not a number is prime is to test, systematically, its divisibility by all the numbers less than its square root. For example, if 1001 were composite, then it would have to be the product of two numbers, a and b, neither of which is one. One of these two numbers would have to be smaller than $\sqrt{(1001)}$ —they can't both be larger— so we need only check for divisors up to 32, which is the square root of the closest square number larger than 1001 (i.e., 1024). Because every number is composed essentially of prime factors, we need only check the prime numbers less than 32; these are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, and 31. This is a feasible number of potential divisors to check.

SECTION 1.5

QUESTIONS ABOUT PRIMES
CONTINUED

There are a number of familiar divisibility tests that can be used to determine if a number is divisible by most of the single digit numbers. One rule that is widely known concerns divisibility by 3: a number is a multiple of 3 if all of its digits sum to a multiple of 3. For example, the digits of 78 sum to 15, and 78 factors to 3×26. What about a number such as 221, which doesn't fall in line with any of the short-cut divisibility tests? To determine whether or not it is prime, using the brute force method described above, we would have to divide it by all of the primes less than its square root, which is somewhere between 14 and 15. Were we to do this, we would find that our first five tries (checking 2, 3, 5, 7, and 11) would be unsuccessful, all yielding remainders. Only on the sixth try (dividing by 13) would we find that 221 is indeed factorable into 13×17.

The brute force method of testing whether or not a number is prime can prove to be quite a headache for large numbers. For example, using a computer that can perform tens of billions of operations per second, the test for a 100-digit number would take about 10^{40} seconds. This is quite a bit longer than the current estimated age of the universe, about 12 billion years.

There are various tests, other than the brute force method, that can tell us about the primeness of larger numbers. One such test uses Wilson's theorem, which states that if a number, p, is prime, then $(p-1)! + 1$ is a multiple of p. For example, we know that the number 7 is prime. Then, according to Wilson's theorem, $(7-1)! + 1 = 6! + 1 = 721$ should be a multiple of 7. Indeed it is: $721 = 7 \times 103$. Unfortunately, as we will see in **Combinatorics Counts**, computing factorials is practically infeasible for large numbers—e.g., 1000! is a number 2,568 digits long, and 1,000,000! is 5.5 million digits long. Wilson's theorem is useless for the sizes of numbers about which the question of primeness has not already been settled.

THE STRUCTURE OF THE PRIMES

- The answer to whether or not there is a pattern behind the primes has eluded mathematicians for millennia.
- One can find interesting examples of both structure and randomness in the primes.

Because directly testing whether or not an arbitrary large number is prime is either very time-consuming or not very reliable, mathematicians have sought to determine the primeness of a number in a totally different way—that is, by looking for a pattern to the primes. If a pattern can be established, then it

SECTION 1.5

QUESTIONS ABOUT PRIMES
CONTINUED

should be possible to determine where primes do and do not occur. Describing exactly where primes should occur on the number line would not only provide an elegant way to know whether or not a number is prime—it would be a beautiful result in itself.

The first person generally credited with attempting to describe a pattern behind the primes was the Greek philosopher and mathematician Eratosthenes. He is credited with creating a method, now called the Sieve of Eratosthenes, for systematically identifying all prime numbers. His method is simple: begin with a finite list of whole numbers and eliminate all the multiples of 2 greater than 2, then all the multiples of 3 greater than 3, then all the multiples of 5 greater than 5, and so on until the only numbers left are the ones that are not multiples of any other numbers: these will be the primes.

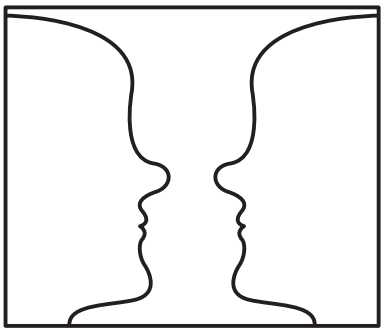
PRIMES ARE WHITE AND COMPOSITES ARE ORANGE

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

This method, however, is not terribly different or better for larger numbers than the brute force method we discussed earlier. It does, however, provide some possible clues to the structure of the primes available to us if, rather than looking at each number individually, we look at the structure as a whole. For example, can we find a pattern behind the primes by focusing on the spacing between them? This strategy is similar to looking at the negative space around a picture instead of looking directly at the picture itself.

SECTION 1.5

QUESTIONS ABOUT PRIMES
CONTINUED


A Cup or two faces?

We can think of the space between primes as "prime deserts," strings of consecutive numbers, none of which are prime. There is a trick, however, for finding prime deserts of whatever length we can think of. For example, $7! = 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 = 5{,}040$. This number is, of course, not prime—but neither is 5,040 + 2, nor 5,040 + 3, nor 5,040 + 4. ... nor 5,040 + 7. In general, for any number N, the string N! + 2, N! + 3,...N! + N identifies a string of N-1 consecutive composite numbers. Setting N = 1,000,000 shows that it is possible to find 999,999 consecutive whole numbers, none of which are prime.

Paradoxically, just as we can find prime deserts of whatever length we choose, we can also find strings of primes—sequences of primes that are evenly spaced on the number line—of whatever length we choose. A good example of strings of primes are the sets called "twin primes." These are pairs of primes that are spaced two numbers apart, such as 11 and 13, or 17 and 19. The set of 3, 5, and 7 forms another such string; again, each number is equally spaced from the others. In yet another example, the numbers 5, 17, 29, 41, and 53 are all prime and are all spaced evenly at 12 numbers apart. Such strings are called arithmetic progressions. In recently completed research done by Terence Tao at UCLA and Ben Green at the University of Bristol, arithmetic progressions of any finite length were proven to exist. Not only are there prime deserts of arbitrary length, but there are also strings of equally spaced primes of whatever finite length we choose. If there is a pattern to the primes, it would have to account for these paradoxically bizarre features.

A tantalizing clue as to the fundamental structure of the primes was discovered by Marin Mersenne, a French music theoretician and mathematician of the 16^{th} and 17^{th} centuries. Specifically, in his study of number theory he became interested in the powers of 2 and found an odd coincidence.

SECTION 1.5

QUESTIONS ABOUT PRIMES
CONTINUED

CHART OF POWERS OF TWO

Powers of 2	2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8
Multiplied out	1	2	4	8	16	32	64	128	256
One less than a power of 2	0	1	3	7	15	31	63	127	255

Notice that, in the above chart, one less than a prime power of 2 yields a prime number. This seems to give us a potential way to predict where prime numbers fall, and it also shows a startling relationship. If the zero power is disregarded, these so-called Mersenne primes appear in the 2^{nd}, 3^{rd}, 5^{th}, 7^{th} , etc. positions in the sequence—in other words, in the prime positions. They are prime numbers in prime positions! Alas, this is but a coincidental occurrence in the smaller numbers, as the pattern does not hold for all prime powers of 2. For example $2^{11} - 1$ is equal to 2,047, which is the product of 89 and 23.

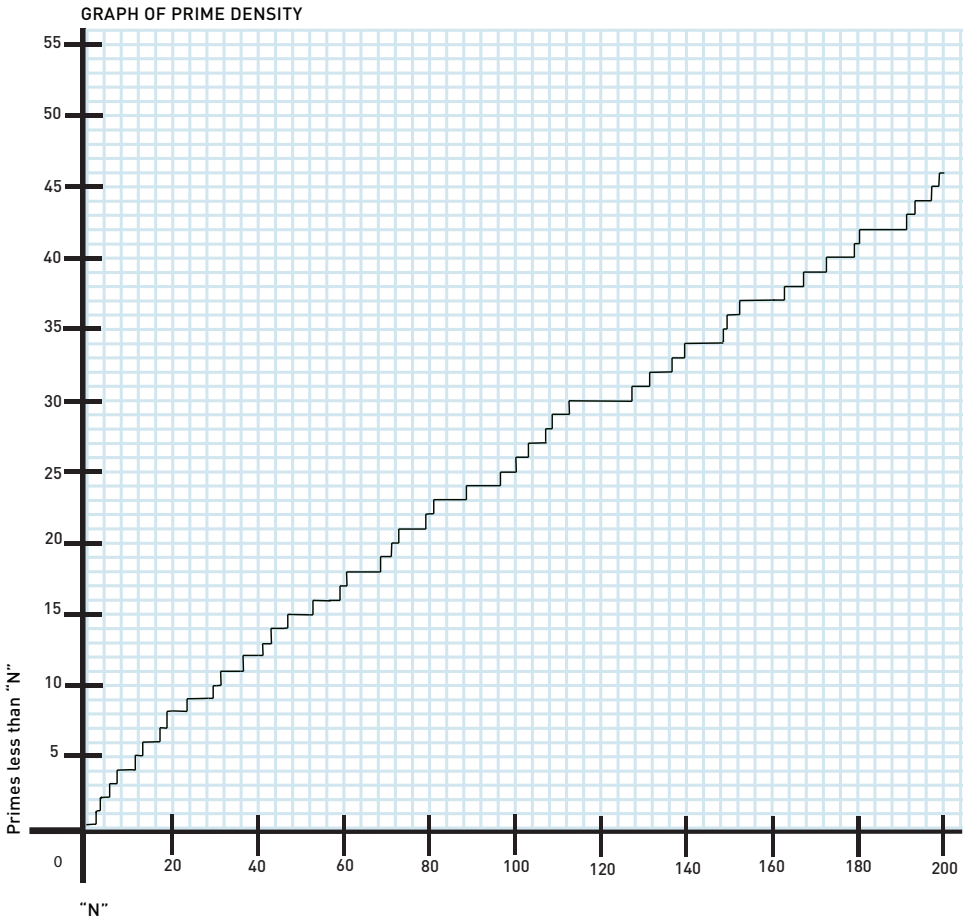
Mersenne primes, nonetheless, are still very important in the modern study of numbers. In fact, the largest prime number that we know about is a Mersenne prime. As of 2006, this number was $2^{32582657} - 1$, a number that is 9,808,358 digits long. It would take an average person more than 100 days just to read it! We should note that in addition to generating non-prime numbers, Mersenne's method also is not guaranteed to predict the positions of all of the primes.

We have so far looked at a few different approaches to predicting where primes should be found on the number line. From the brute force method of Eratosthenes to the elegant ideas of Tao, Green, and Mersenne, we have seen that the primes do not give up their secrets easily. Perhaps, in asking where exactly each prime falls on the number line, we are asking the wrong question.

Gauss, of fundamental theorem of arithmetic fame, took a different approach. Finding a straightforward attack daunting, he examined matters from a different perspective. He examined the density of primes below a certain number.

SECTION 1.5

QUESTIONS ABOUT PRIMES
CONTINUED



He found that the density of primes—that is, a measure of the number of primes in relation to all the numbers below any given number—is fairly constant. By looking at tables of the number of primes below a given number, *n*, Gauss observed that this measure always seems to be approximately the ratio $\frac{n}{\log n}$, which implies that the n^{th} prime is approximately n log n. This finding, while not exactly what we were looking for in terms of predicting where primes appear on the number line, represents a significant result in the search for a "law of the primes."

RIEMANN'S HYPOTHESIS

- Riemann, following in the footsteps of Euler, thought that the pattern of the primes was tied to the zeta function, which is a generalization of the harmonic series.

SECTION 1.5

QUESTIONS ABOUT PRIMES
CONTINUED

Gauss's conjecture about the distribution of the primes was an important first step. By looking at the problem from a different perspective, that of prime density, and by examining functions that would give not a prime number directly, but rather the density of primes below a specified number, Gauss opened the exploration of the primes to new disciplines of mathematics. He was not the only one working on this problem, however. The Swiss mathematician Leonhard Euler, working in a similar vein, introduced yet another approach to discovering a pattern behind the primes.

Euler was fascinated by a relative of the harmonic series known as the zeta function. The harmonic series is simply the sum of the reciprocals of all the whole numbers.

$$\sum_{k=1}^{\infty}\frac{1}{k} \qquad 1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}+\ldots$$

What tipped Euler off that the harmonic series' cousin, the zeta function, might be useful in exploring the structure of the primes was that it contains every natural number.

$$V(x)=1+\frac{1}{2^x}+\frac{1}{3^x}+\frac{1}{4^x}\ldots=\sum_{n=1}^{\infty}\frac{1}{n^x}$$

Notice that the zeta function expresses the sum of the reciprocals of the x^{th} power of every number. We can input any value we choose for x and study the behavior of the series. For any value of x less than or equal to one, the series diverges—grows infinitely large. For values of x greater than one, the series converges to a finite value. However, just because we know that the series converges does not mean that we can always find the value upon which it settles.

Euler played with the zeta function and found that he was able to express every element of the infinite sum as a product of the reciprocals of prime numbers. This insight tied the study of prime numbers to the study of infinite series and paved the way for one of the most elusive hypotheses in mathematics.

$$V(x)=\frac{1}{1^x}+\frac{1}{2^x}+\frac{1}{3^x}+\ldots+\frac{1}{n^x}\ldots$$

SECTION 1.5

EULER'S FACTORIZATION

QUESTIONS ABOUT PRIMES
CONTINUED

$$=(1+\frac{1}{2^x}+\frac{1}{4^x}+\ldots)\times(1+\frac{1}{3^x}+\frac{1}{9^x}+\ldots)\times\ldots\times(1+\frac{1}{p^x}+\frac{1}{(p^2)^x}+\ldots)\times\ldots$$

Bernhard Riemann, one of the most influential mathematicians of the 19th century, built upon Euler's discovery, specifically exploring the consequences of using complex, or imaginary, numbers as the inputs to Euler's version of the zeta function. This effectively constructed a larger landscape of numbers to explore, one that gave a better perspective on how the elusive primes might be distributed along the number line. Riemann proposed that the distribution of the primes was tied to the zeroes of the zeta function when considered over the complex numbers.

If you imagine the entire collection of complex numbers to be a landscape with hills and valleys, the zeta function is like a road that traverses it. We can think of the zeroes of the zeta function as being the points at which the elevation of the road is at sea level. Riemann said that these points mark where the primes should occur.

Riemann's hypothesis was groundbreaking, but it remains a hypothesis, unproven, to this day. Given the history of the problem it purportedly solves, and the centuries of effort that have led to it, the proof of Riemann's hypothesis will be quite valuable. As of this writing, there is a $1,000,000 reward available to any person who shows definitively whether or not it is true or untrue.

The preceding discussion should have given you a sense that primes are intrinsically fascinating. They are the fundamental basis of arithmetic—yet, they are extremely mysterious. They surprisingly represent both the most basic and the most cutting-edge aspects of mathematics. On a daily basis, however, we are not typically conscious of them. Because of this, it is tempting to believe that playing with primes is the purview of pure mathematics, with little relevance to our daily lives. This couldn't be further from the truth, especially in our modern age when numbers are used to transmit all types of information, the security of which is of great importance. Primes provide the building blocks of encryption schemes that protect our most sensitive and valuable data.

SECTION 1.6

ENCRYPTION

- History
- Caesar Ciphers
- Modular Arithmetic
- Prime Moduli

HISTORY

- The need to send private messages has ancient roots.
- Most historical encryption schemes used private keys.

When sending sensitive information, such as logging onto a bank account via the World Wide Web, we want the intended receiver to be able to "read" the message, and we also want any unintended recipient (or thief) of the message to be thwarted. To accomplish this, we need a system of encryption, one that will be impervious to even the cleverest of hackers. Online transactions are only the most recent example of situations in which information must be protected while in transit. There have been many different systems of encoding throughout the years, many of them mathematical in nature.

Mathematical encryption relies on concepts such as modular arithmetic and the fundamental properties of prime numbers to make messages incomprehensible to unintended recipients. Obviously, encryption requires operations that are easy to perform one way (i.e., encoding), yet nearly impossible to perform the other way (i.e., decoding) without a key. Prime numbers can help us with this. Recall that multiplying two primes is easy, whereas factoring a product of two unknown primes can be extremely difficult and time-consuming.

The problem of sending a vital message to someone without it being discovered, or deciphered, is an ancient one. This need crops up in a variety of situations, but an all-too-common need for encryption has arisen time after time on the battlefield. When attacking an enemy, it is critical to be able to send coordinating information to your involved units without the enemy discovering your plans. By encrypting messages in some fashion, you hope that, even if a message is intercepted, its message will be inaccessible to unintended readers.

Encryption schemes have come in many forms throughout the ages. Many early schemes could hardly be called "encryption"—"concealment" would be a more appropriate term. A particularly striking example is the story of Histaiaeus, a

SECTION 1.6

ENCRYPTION
CONTINUED

5th-century-BC Greek provincial ruler, or tyrant, who wanted to encourage a fellow tyrant of a neighboring state to revolt against the Persian king, Darius. To convey his instructions securely, Histaiaeus shaved the head of his messenger, wrote the message on his scalp, and then waited for the hair to re-grow. The messenger, apparently carrying nothing of interest, traveled without being harassed. Upon arriving at his destination, the messenger shaved his head and pointed it toward the intended recipient. Although this was perhaps clever for its time, such a system would quickly be compromised as word of its use spread.

CAESAR CIPHERS

- The simplest encryption scheme is to jumble the letters of the alphabet according to some rule.

Clearly, a system of simply concealing one's message is effective only up to a point—a thorough search is all that is needed to expose the scheme and intercept the message. To ensure message security, one would want an interloper, were he or she to find the communication, to be baffled by what it actually says. A simple scheme, whose first use is attributed to Julius Caesar, is to replace each letter of the alphabet with a different letter according to some rule. For example:

CAESAR CIPHER USING RULE OF "ADD THREE"

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

This scheme replaces each letter with the letter that comes three letters later in the sequence of the alphabet. In effect, this encoding scheme just shifts the alphabet three letters to the left, with the substitutions for the last three letters coming from the beginning of the sequence. Our key, let's call it "k," is 3. Let's now shift our thinking from letters to numbers; we can easily assign each letter of the alphabet to a corresponding number as follows:

CAESAR CIPHER CORRESPONDING LETTERS TO NUMBERS

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

SECTION 1.6

ENCRYPTION
CONTINUED

Applying the same "shift by 3" that was just used in the preceding example to this new system creates the following encryption scheme:

CAESAR CIPHER WITH NUMBERS SHIFTED THREE PLACES

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3

To encrypt a letter, we simply add three to the number with which it was originally paired. For example:

A, originally paired with "1" gets shifted, or encrypted, to "4."
and
M, originally paired with "13" gets shifted to "16."

When we get to X, however, we have a problem. Following the current encryption scheme, X, originally associated with "24," would get shifted to "27." However, 27 isn't anywhere in our list of possible numbers. So, we can wrap around and start over at 1 after hitting 26 instead of using more numbers. To express this adjustment mathematically, we could write:

$24 + 3 = 1$

This strange sort of arithmetic might seem somewhat familiar because it is related to how we apply arithmetic to cyclical time. For example, if it is four o'clock and we add twelve hours, it is again four o'clock, ignoring the A.M./P.M. difference. This "clock math" is known as "modular arithmetic."

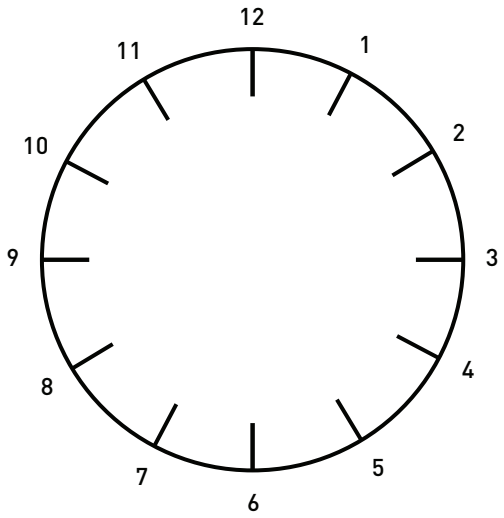
SECTION 1.6

ENCRYPTION
CONTINUED

MODULAR ARITHMETIC

- Modular arithmetic is math that incorporates "wrap-around" effects.

Modular arithmetic is a key to understanding modern forms of encryption, and it also demonstrates interesting properties of prime numbers. It incorporates "wrap around" effects by having some number other than zero play the role of zero in addition. For example, on an analog clock:



The number 12 behaves like zero, because adding 12 hours to any time (again, ignoring A.M. or P.M. differences) doesn't change anything. A typical addition problem in this scheme would be:

$3 + 12 = 3$

To write a number in this system, we have to be conscious of how many multiples of 12 it contains. A number such as 5 has no multiples of 12 in it, so we would simply write 5. The number 17, however, is 5 + 1(12), which is also equal to 5 in this system. Similarly, the number 29 is 5 + 2(12), which is also equal to 5, again because the number twelve is acting like zero in this system. In such a system, 12 is called the "modulus." To describe the number 29, we would say that it is "congruent to 5 modulo 12", or $29 \equiv 5 \bmod 12$.
Note that:
$5 \equiv 5 \bmod 12$
$17 \equiv 5 \bmod 12$
$29 \equiv 5 \bmod 12$
etc.
Any number of the form $5 + n(12)$ will be congruent to 5 in this system.